Administrative Policies and Procedures: 7.2

Subject:	**Acceptable Use, Network Access Rights and Obligations**
Authority:	TCA 37-5-105, 37-5-106; TCA Section 435501, et seq., effective May 10, 1994; TCA, Section 107512, Effective July 1, 2000; TCA Section 107504, effective July 1, 2001
Standards:	None
Application:	To All Department of Children's Services Employees and Individuals who have been provided access rights to the State of Tennessee networks, State provided e-mail, and/or Internet agency issued network or system User ID's.

Policy Statement:

The Department of Children's Services shall comply with the Department of Finance and Administration – Office of Information Resources policies and procedures regarding computer network access and usage.

Purpose:

To establish guidelines for State-owned hardware and software, computer network access and usage, Internet and e-mail usage, telephone, and security and privacy for users of the State of Tennessee Wide Area Network.

Procedures:

A. Objectives

1. Ensure the protection of proprietary, personal, privileged, or otherwise sensitive data and resources that may be processed in any manner by the State, or any agent for the State.
2. Provide uninterrupted network resources to users.
3. Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
4. Maintain security of and access to networked data and resources on an authorized basis.
5. Secure email from unauthorized access.
6. Protect the confidentiality and integrity of files and programs from unauthorized users.
7. Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.
8. Provide Internet and email access to the users of the State of Tennessee networks.

B. Network Resources uses and prohibitions	1. State employees, vendors/business partners/subrecipients, local governments, and other governmental agencies may be authorized to access state network resources to perform business functions with or on behalf of the State. 2. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement. 3. It is recognized that there may be incidental personal use of State Network Resources. This practice is not encouraged and employees should be aware that all usage may be monitored and that there is no right to privacy. Various transactions resulting from network usage are the property of the state and are thus subject to open records laws. 4. Prohibited uses of network resources include but are not limited to: a) Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation. b) Installing software that has not been authorized by the Office of Information Systems. c) Attaching processing devices that have not been authorized by the Office of Information Systems. d) Using network resources to play or download games, music or videos that are not in support of business functions. e) Leaving workstation unattended without engaging password protection for the keyboard or workstation. f) Using network resources in support of unlawful activities as defined by federal, state, and local law. g) Utilizing network resources for activities that violate conduct policies established by the Department of Personnel or the Agency where the user is employed or under contract.
C. E-mail uses and prohibitions	1. Email and calendar functions are provided to expedite and improve communications among network users. 2. Prohibited uses of e-mail include but are not limited to sending: a) Unsolicited junk email or chain letters (e.g. “spam”) to any users of the network. b) Any material that contains viruses or any other harmful or deleterious programs. c) Copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher. d) Communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.

	e) Confidential material to an unauthorized recipient, or sending confidential email without the proper security standards (including encryption if necessary) being met. 3. Email created, sent or received in conjunction with the transaction of official business are public records in accordance with *T.C.A 107301 through 107308*, and the rules of the Public Records Commission. 4. State records are open to public inspection unless they are protected by State or Federal law, rules, or regulations. Because a court could interpret state records to include draft letters, working drafts of reports, and what are intended to be casual comments, be aware that anything sent as electronic mail could be made available to the public.
D. Internet access	1. Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions. 2. Prohibited uses include, but are not limited to, using: a) The Internet to access non-State provided web email services. b) Instant Messaging or Internet Relay Chat (IRC). c) The Internet for broadcast audio for non-business use. d) The Internet when it violates any federal, state or local law.
E. Statement of consequences	Noncompliance with this policy may constitute a legal risk to the State of Tennessee, an organizational risk to the State of Tennessee in terms of potential harm to employees or citizen security, or a security risk to the State of Tennessee's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.
F. Statement of enforcement	Noncompliance with this policy may result in the following immediate actions: 1. Written notification will be sent to the Commissioner and to designated points of contact in the DCS Offices of Human Resources, Information Systems and Inspector General to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, sub-recipient, or contractor, the contract administrator will also be notified. 2. User access may be terminated immediately by the Security Administrator, and the user may be subject to subsequent review and action as determined by the department or contract administrator.

Forms:	*None*
Collateral documents:	***Department of Finance and Administration – Office of Information Resources Acceptable Use Policy*** ***Tennessee Computer Crimes Act***

Glossary:	
Public records:	*"Public record(s)" or "state record(s)"* are all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (*T.C.A. 107301(6)*.